IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

Huawei Technologies USA, Inc., and Huawei Technologies Co., Ltd., Plaintiffs, v. The United States of America, Emily Webster Murphy, Administrator of the General Services Administration, Alexander Acosta, Secretary of Labor, Alex Azar II, Secretary of Health and Human Services, Betsy DeVos, Secretary of Education, Sonny Perdue, Secretary of Agriculture, Robert Wilkie, Secretary of Veterans Affairs, and David L. Bernhardt, Acting Secretary of the Interior, in their official capacities, Defendants.	§ §	Civil Action No. _____

COMPLAINT

Plaintiffs Huawei Technologies USA, Inc., and Huawei Technologies Co., Ltd. (collectively, "Plaintiffs" or "Huawei"), by and through their attorneys, bring this action under the United States Constitution and 28 U.S.C. §§ 1331, 2201, and 2202, seeking a declaration that

pertinent provisions of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 ("NDAA" or "2019 NDAA"), that define certain equipment and services produced or provided by Huawei Technologies Co., Ltd. and its subsidiaries and affiliates as "covered telecommunications equipment or services," *id.* § 889(f)(3)(A), (C), and consequently restrict the procurement and use of such equipment by executive agencies, federal government contractors, and federal loan and grant recipients, *id.* § 889(a)-(b), are unconstitutional. Plaintiffs also seek an injunction and any other appropriate relief. In support thereof, Plaintiffs allege as follows:

PRELIMINARY STATEMENT

1. The Framers of the United States Constitution were deeply concerned about the potential abuse of legislative power. They believed that "[t]he legislative department is everywhere extending the sphere of its activity, and drawing all power into its impetuous vortex," and that as a result, "[i]t is against the enterprising ambition of this department that the people ought to indulge all their jealousy and exhaust all their precautions." The Federalist No. 48 (James Madison). The Framers accordingly granted Congress only limited and enumerated legislative powers; divided these powers between a House of Representatives and a Senate; subjected the exercise of these powers to strict procedures; and vested the executive and judicial powers in separate, independent branches of the government.

2. One of the Framers' particular concerns was that the legislature would use its power to target specific individuals for adverse treatment. The Framers believed that, if the legislature could itself sanction specific persons "without hearing or trial" conducted by the Executive or the courts, "no man can be safe, nor know when he may be the innocent victim of a prevailing faction." 3 The Papers of Alexander Hamilton, at 485–86 (Harold C. Syrett ed. 1961–

1979). Thus, even where the Framers otherwise granted Congress enumerated legislative powers, they prohibited it from using those powers to enact bills of attainder that impose punishment on specific individuals identified by the legislature. Further, through the Due Process Clause, they prohibited legislation that would single out particular persons for deprivations of liberty. Finally, through the Vesting Clauses and the resulting separation of powers, the Framers prohibited legislation that, rather than simply enacting a general rule, applied a rule to an individual case or person.

3. Provisions of section 889 of the 2019 NDAA violate these constitutional limitations. In particular, section 889 specifically targets Plaintiff Huawei Technologies Co., Ltd., and its subsidiaries and affiliates, such as Plaintiff Huawei Technologies USA, Inc. Section 889 calls out Huawei by name, legislatively adjudicates it to be connected to the Government of the People's Republic of China, and precludes U.S. government agencies not only from purchasing specified Huawei equipment and services, but also from contracting with or awarding grants or loans to third parties who purchase or use such equipment or services—regardless of whether the equipment or services have any impact on or connection to the government of the United States. The actual and intended effect of these prohibitions is to bar Huawei from significant segments of the U.S. market for telecommunications equipment and services, thereby inflicting immediate and ongoing economic, competitive, and reputational harms on Huawei.

4. Section 889 permanently imposes these burdens and sanctions on Huawei without giving it a fair hearing or the opportunity to rebut the allegations against it, and without opportunity for escape. The statute specifically and expressly applies these broad prohibitions and sanctions only to Huawei and one other named entity. In contrast, the statute gives the Secretary of Defense, in consultation with the FBI Director or the Director of National

Intelligence, authority to determine whether other entities are owned or controlled by, or otherwise connected to, the Chinese government—determinations that are then subject to judicial review under the Administrative Procedure Act. The statute affords those Officers of the United States the discretion to change their determinations if they find, for example, that the facts about a particular entity have changed. But those Officers have no such discretion with respect to Huawei: even if those Officers definitively find that Huawei has no connection to the Chinese government, the prohibitions targeting, and sanctions imposed on, Huawei will remain in place. In short, section 889 blacklists Huawei and bars it from significant sectors of the U.S. telecommunications market, all without giving Huawei a fair hearing at which it could be informed of and confront the accusations made against it.

5. In so doing, section 889 violates at least three constitutional provisions: It violates the Bill of Attainder Clause by singling out Huawei for punishment—blacklisting it, impugning both its general reputation and its specific commitment to honoring the laws of the United States, and denying it any procedure through which it can clear its name and escape sanction. Section 889 also violates the Due Process Clause by selectively depriving Huawei of its liberty—severely curtailing its freedom to do business, stigmatizing it by effectively branding it a tool of the Chinese government and a risk to U.S. security, and denying it any pre-deprivation legal process to confront the congressional charges against it. And section 889 violates the Vesting Clauses and the resulting separation of powers by legislatively adjudicating Huawei to be "guilty" of an alleged connection to the Chinese government, and by implication a threat to U.S. security, rather than leaving it to the Executive and the courts to make and adjudicate any such charges.

6. Moreover, as a practical matter, section 889's focus on Huawei (and one other company), apparently based on Huawei Technologies Co., Ltd.'s national origin, makes no sense. Section 889 permits manufacturers with extensive operations in China and joint venture agreements with the Chinese government to continue to sell equipment to the U.S. Government and its contractors and grant and loan recipients, while legislatively singling out Huawei—a private, non-government-owned company controlled by a private Board of Directors—and just one other entity for sweeping adverse treatment. Further, the government itself has recognized that virtually *all* manufacturers of telecommunications equipment in the world face cybersecurity risks as a result of vulnerabilities in the global supply chain. Yet section 889 does nothing to address these global supply chain risks. Thus, if the central purpose of section 889 is to prevent Chinese-origin equipment from being used, directly or indirectly, by the U.S. Government, the provision is ineffective on its face. Moreover, it is overbroad, because it bars use (by government contractors) or purchase (by government grant and loan recipients) of Huawei equipment and services even where Huawei equipment or services are not being used to support a government-related function.

7. In short, Section 889 is not only contrary to the economic interests of the United States and its citizens, and ineffective at advancing U.S. security interests, it is also contrary to the Constitution of the United States. Huawei is a world-leading provider of information and communications technology products and services, offering more advanced equipment at lower costs than any other such company, and doing so in areas of the world and of the United States that other providers serve less effectively or not at all. Without Huawei equipment and services, consumers in the United States (particularly in rural and poor areas) will be deprived of access to the most advanced technologies, and will face higher prices and a significantly less competitive

market. In the area of 5G mobile service in particular, American consumers will have reduced access to state-of-the art networks and suffer from inferior service. At the same time, Huawei equipment and services are subject to advanced security procedures, and no backdoors, implants, or other intentional security vulnerabilities have been documented in any of the more than 170 countries in the world where Huawei equipment and services are used. Moreover, while there are real risks in the global supply chain that can and should be addressed by comprehensive supply chain strategies and rules, those risks are not rationally or effectively addressed by singling out and blacklisting equipment of specific companies such as Huawei. Indeed, as noted, Huawei is a privately-owned company controlled by a private Board of Directors. While courts do not have the authority to protect the people from all the ill-advised aspects of the NDAA, they do have the duty to protect Huawei and others from its unconstitutional aspects—including its specific targeting of Huawei for punishment, its deprivation of Huawei's liberty without a fair and impartial hearing, and its usurpation of the charging and adjudicative powers reserved by the Constitution to the executive and judicial branches. Plaintiffs respectfully request that the Court declare unconstitutional and enjoin enforcement of those discrete aspects of section 889 that violate the Constitution, while leaving all other aspects of the NDAA, and the remainder of section 889 itself, intact.

THE PARTIES

A. Plaintiffs

8. Plaintiff Huawei Technologies USA, Inc. ("Huawei USA"), is a corporation organized under Texas law with headquarters at 5700 Tennyson Parkway #500, in Plano, Texas, 75024.

9. Plaintiff Huawei Technologies Co., Ltd. ("Huawei Technologies"), is a limited liability company organized in Shenzhen, Guangdong Province, with headquarters at Huawei Industrial Base, Shenzhen 518129, in the People's Republic of China.

10. Plaintiffs Huawei USA and Huawei Technologies are wholly-owned subsidiaries of Huawei Investment & Holding Co. Ltd. ("Huawei Investment"), and are therefore affiliates. In addition, plaintiff Huawei USA is an indirect subsidiary of plaintiff Huawei Technologies.

11. Huawei Investment is a resident of China and has its corporate headquarters at Huawei Industrial Base, Shenzhen 518129, People's Republic of China.

12. Huawei Investment is a private company wholly owned by its employees. Its direct shareholders are an employee-stock-ownership plan named the Union of Huawei Investment & Holding Co., Ltd., and the founder of Huawei, Mr. Ren Zhengfei. The Union of Huawei Investment & Holding Co., Ltd. involved more than 97,000 employees as of February 2019. Mr. Ren's investment accounted at that time for only approximately 1.14% of Huawei Investment's total share capital.

B. Defendants

13. The United States of America is a defendant based on the actions of the United States Congress in enacting the NDAA, and because it is a proper defendant under 5 U.S.C. § 702.

14. Defendant Emily Webster Murphy is the Administrator of the General Services Administration (GSA). She is sued in her official capacity.

a. Defendant Murphy leads the General Services Administration in its mission of providing centralized procurement for the federal government. GSA's responsibilities include drafting and administering the Federal Acquisition Regulation, which applies to all executive agency acquisitions, subject to

certain exceptions. *See* 41 U.S.C. §§ 1121, 1303(a)(1); 48 C.F.R. ch. 1. Section 889 of the NDAA directs the heads of federal executive agencies to take or refrain from taking certain actions with regard to government contracts, including contracts subject to the Federal Acquisition Regulation.

b. The NDAA directs Defendant Murphy to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between GSA and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to any loans or grants awarded by GSA to entities that use certain equipment, systems, or services provided by Huawei. Defendant Murphy is a proper defendant under 5 U.S.C. § 702.

15. Defendant Alexander Acosta is the Secretary of Labor. He is sued in his official capacity. The NDAA directs Defendant Acosta to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of Labor and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to loans or grants awarded by the Department of Labor to entities that use certain equipment, systems, or services provided by Huawei. Defendant Acosta is a proper defendant under 5 U.S.C. § 702.

16. Defendant Alex Azar II is the Secretary of Health and Human Services. He is sued in his official capacity. The NDAA directs Defendant Azar to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of Health and Human Services and any entities that use certain equipment, systems, or services provided by

Huawei; and with regard to loans and grants awarded by the Department of Health and Human Services to entities that use certain equipment, systems, or services provided by Huawei. Defendant Azar is a proper defendant under 5 U.S.C. § 702.

17. Defendant Betsy DeVos is the Secretary of Education. She is sued in her official capacity. The NDAA directs Defendant DeVos to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of Education and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to loans and grants awarded by the Department of Education to entities that use certain equipment, systems, or services provided by Huawei. Defendant DeVos is a proper defendant under 5 U.S.C. § 702.

18. Defendant Sonny Perdue is the Secretary of Agriculture. He is sued in his official capacity. The NDAA directs Defendant Perdue to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of Agriculture and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to loans and grants awarded by the Department of Agriculture to entities that use certain equipment, systems, or services provided by Huawei. Defendant Purdue is a proper defendant under 5 U.S.C. § 702.

19. Defendant Robert Wilkie is the Secretary of Veterans Affairs. He is sued in his official capacity. The NDAA directs Defendant Wilkie to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of Veterans Affairs and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to loans and grants awarded by the Department of Veterans Affairs to entities that use

certain equipment, systems, or services provided by Huawei. Defendant Wilkie is a proper defendant under 5 U.S.C. § 702.

20. Defendant David L. Bernhardt is the Acting Secretary of the Interior. He is sued in his official capacity. The NDAA directs Defendant Bernhardt to take or refrain from taking certain actions with regard to the procurement of certain equipment, systems, or services produced or provided by Huawei; with regard to contracts between the Department of the Interior and any entities that use certain equipment, systems, or services provided by Huawei; and with regard to loans or grants awarded by the Department of the Interior to entities that use certain equipment, systems, or services provided by Huawei. Defendant Bernhardt is a proper defendant under 5 U.S.C. § 702.

CONSTITUTIONAL PROVISIONS

21. This action arises under the United States Constitution's Bill of Attainder Clause, art. I, § 9, cl. 3, the Due Process Clause of the Constitution's Fifth Amendment, *id.* amend. V, and the Constitution's Vesting Clauses and resulting separation of powers, *see id.* art. I, § 1 (legislature); *id.* art. II, § 1, cl. 1 (executive); *id.* art. III, § 1 (judiciary).

22. The Bill of Attainder Clause states: "No Bill of Attainder . . . shall be passed." *Id.* art. I, § 9, cl. 3.

23. The Due Process Clause of the Fifth Amendment provides: "No person shall . . . be deprived of life, liberty, or property, without due process of law." *Id.* amend. V.

24. The Constitution's Vesting Clauses and resulting separation of powers grant Congress only limited, enumerated "legislative powers," and place the "executive" and "judicial" powers in the President and the courts, respectively. *See id.* art. I, § 1 (legislature); *id.* art. II, § 1, cl. 1 (executive); *id.* art. III, § 1 (judiciary).

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under the United States Constitution.

26. The Court has authority to grant declaratory and injunctive relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*; 5 U.S.C. § 702; and the Court's inherent equitable powers.

27. Under federal common law, a party may sue "to enjoin unconstitutional actions by . . . federal officers," *Armstrong v. Exceptional Child Ctr., Inc.*, 135 S. Ct. 1378, 1384 (2015); *see id.* (citing *Am. Sch. of Magnetic Healing v. McAnnulty*, 187 U.S. 94, 110 (1902)), and no waiver of sovereign immunity is necessary, because sovereign immunity does not apply in such circumstances. *E.g.*, *Dugan v. Rank*, 372 U.S. 609, 621–22 (1963). Furthermore, the United States has waived its sovereign immunity pursuant to 5 U.S.C. § 702.

28. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e)(1)(C), because the United States and officers or employees of agencies of the United States acting in their official capacities are defendants, and because Plaintiff Huawei USA has its principal place of business in this district, based on its headquarters in Plano, which is located within this district. No real property is involved in this action.

FACTUAL ALLEGATIONS

I. BACKGROUND ON HUAWEI

A. Overview Of Huawei Technologies

29. Huawei Technologies is a global leader in information and communications technology products and services. It was established in 1987 in Shenzhen, Guangdong Province, a special economic zone where market-oriented reforms were first introduced in China.

30. Huawei Technologies is owned by its founder and employees (via an employee-stock-ownership plan), and is controlled by its Board of Directors, all 17 members of which are private citizens who hold no positions in the Chinese government. Huawei Technologies (and its parent Huawei Investment) has no Chinese government ownership.

31. Huawei Technologies produces, among other things, products (including routers and layer 3 switches) that are capable of routing or redirecting user data traffic.

B. Overview Of Huawei USA

32. Plaintiff Huawei USA employs approximately 250 employees and provides information and communications technology equipment and services to 85 active U.S. wireline and wireless carriers and numerous enterprise customers, which include U.S. corporations, schools, and other institutions.

33. Huawei USA has a Board of Directors. None of the board members hold any positions in the Chinese government. Huawei USA's Board is responsible for, among other things, overseeing and managing the business of the corporation and setting policy to be implemented by the officers of the corporation; approving and directing the officers of the corporation to implement the development strategy and business plans of the corporation; and nominating, appointing, dismissing, and evaluating the performance of senior management. Huawei USA has no Chinese government ownership.

34. Huawei USA markets and sells, among other things, products (including routers and layer 3 switches) that are capable of routing or redirecting user data traffic.

II. U.S. GOVERNMENT INVESTIGATION OF THE GLOBAL CYBERSECURITY THREAT

35. The government of the United States has been taking steps to identify and mitigate cybersecurity risks—including, in particular, supply chain risks—for more than twenty years.

a. In 1998, President Clinton issued a directive setting forth "the policy of the United States to assure the continuity and viability of critical infrastructures" such as telecommunications networks by eliminating their vulnerabilities to both physical and cyber attacks. The White House, Presidential Decision Directive/NSC-63, at 2 (May 22, 1998), https://fas.org/irp/offdocs/pdd/pdd-63.pdf.

b. In 2002, Congress passed the Federal Information Security Management Act (FISMA), which required the development of minimum standards for the security of federal information systems. 40 U.S.C. § 11331. Pursuant to FISMA, the National Institute of Standards and Technology (NIST) developed two standards, one of which as of 2009 specifically requires government agencies to take measures to protect their supply chains. Gov't Account. Office, IT Supply Chain, at 7–9 (2012), https://bit.ly/2CnBuUe.

c. In 2003, the Executive Branch released the first national cybersecurity strategy, which identified telecommunications as a critical infrastructure that the Government must protect from cyberattack. The White House, Nat'l Strategy to Secure Cyberspace, at 1, 4, 33–34 (Feb. 2003), https://bit.ly/1GxRVq6.

d. In 2008, President Bush launched the Comprehensive National Cybersecurity Initiative (CNCI), which called for a "detailed strategy and implementation plan to better manage and mitigate supply chain vulnerabilities." The White House, Nat'l Sec. Presidential Directive NSPD-54/Homeland Sec. Presidential Directive HSPD-23, at 11–12 (Jan. 8, 2008), https://bit.ly/2CUu7oA.

e. In February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a review in order to develop a strategic framework to coordinate and integrate government plans and activities addressing cyber risks. The White House, Fact Sheet: Cyberspace Policy Review (May 29, 2009), https://fas.org/irp/news/2009/05/cyber-fs.html. The resulting report recognized that "the emergence of new centers for manufacturing, design, and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations," and called for "[a] broad, holistic approach to risk management . . . rather than a wholesale condemnation of foreign products and services." The White House, Cyberspace Policy Review, at 34 (May 29, 2009), https://fas.org/irp/eprint/cyber-review.pdf.

f. In May 2009, President Obama accepted the recommendations of the report and subsequently refined the CNCI into twelve initiatives, one of which called for a "multi-pronged approach" to addressing "[r]isks stemming from both the domestic and globalized supply chain . . . in a strategic and comprehensive way over the entire lifecycle of products, systems and services." The White House, The Comprehensive National Cybersecurity Initiative,

https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative. In this initiative, the President recognized that "[m]anaging this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices." *Id.*

g. In 2012, the Director of National Intelligence testified before Congress that "[c]yber threats pose a critical national and economic security concern," and that one of the "greatest strategic challenges regarding cyber threats" was mitigating "the highly complex vulnerabilities associated with the IT supply chain for US networks." James R. Clapper, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, at 7–8 (Jan. 31, 2012), https://bit.ly/2J5gtiJ.

h. In 2018, NIST released a new version of its cybersecurity framework that provided further guidance on how organizations (including government agencies) should assess and manage cyber supply chain risks. Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity, at 15–17, 28–29 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The framework explains that

steps to mitigate cyber supply chain risks may include determining cybersecurity requirements for suppliers, enacting those requirements through mechanisms such as contracts, and verifying that those requirements are being met through various assessment methodologies. *Id.*

i. Also in 2018, the Department of Homeland Security set up an interagency Supply Chain Task Force to "examine and develop consensus recommendations for action to address key strategic challenges to identifying and managing risk associated with the global ICT supply chain and related third-party risk." Dep't of Homeland Sec., ICT Supply Chain Task Force Fact Sheet (July 31, 2018), https://bit.ly/2Ctftnl. The task force is "intended to focus on potential near- and long-term solutions to manage strategic risks through policy initiatives and opportunities for innovative public-private partnership." *Id.*

j. In addition, in December of 2018, Congress passed and the President signed the SECURE Technology Act, which incorporated the Federal Acquisition Supply Chain Security Act of 2018. This Act requires development of government-wide criteria and rules for identifying, assessing, and mitigating supply chain risks posed by any global supplier to the government. It also provides procedural protections to suppliers potentially excluded from a procurement, such as notice, opportunity for rebuttal, and judicial review.

36. In taking the steps described in Paragraph 35, the Executive Branch (and, sporadically, Congress) recognized that supply chains are global, and did not claim, pretend, or suggest that cybersecurity risks could be meaningfully addressed by taking targeted action aimed

only at particular companies. The White House, Nat'l Cyber Strategy, at 26 (Sep. 2018), https://bit.ly/2xrQ0XK; Framework for Improving Critical Infrastructure Cybersecurity, at 15–17 ("Supply chains are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations."); Dep't of Homeland Sec., ICT Supply Chain Task Force Fact Sheet. Rather, as NIST has explained, information and communications-technology "products . . . or services originating anywhere (domestically or abroad) might contain vulnerabilities that can present opportunities for . . . supply chain compromises." Nat'l Inst. of Standards & Tech., NIST Special Publication 800-191, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, at 1–2 (Apr. 2015), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

37. Consistent with this approach, experts have recognized that the global telecommunications supply chain is complex and dynamic, and that security risks arise from the cumulative supply chain—not the vendor whose name happens to appear on the finished product. Accordingly, identifying risk requires, among other steps, an individualized analysis of who develops and manufactures particular equipment, its components, and software; where that work takes place; the arrangements under which the work happens (for example, joint ventures with state-owned enterprises, or manufacturing by wholly-owned subsidiaries); and the ability of a foreign state or other malicious actor to introduce backdoors or other vulnerabilities given these factors.

38. With respect to supply chain risk related to China in particular, telecommunications companies other than Huawei are owned by Chinese investors; and numerous other companies have manufacturing facilities in China, embed components imported from China, use software written by Chinese programmers, or have other ties to China. For

example, two major telecommunications companies operate joint ventures with the Chinese government and manufacture equipment in China.[1] Non-Chinese firms in the telecommunications equipment sector that operate in China or have joint ventures with the Chinese government are also subject to Chinese laws and regulatory authority.

III. CONGRESSIONAL INTERFERENCE WITH HUAWEI'S U.S. BUSINESS

39. Despite this recognition of the broad and interconnected nature of global supply chain risk by the Executive Branch (and, sporadically, Congress), Congress has over the past several years focused most of its energy in this sphere on singling out individual companies for adverse treatment in a way that fails to reflect the dispersed nature of the global supply chain. Rather than concentrating on developing the "broad, holistic approach to risk management" recommended by the Executive Branch, Congress has instead chosen to engage in the "wholesale condemnation" of particular "foreign products and services" that the Executive had warned against. *See* Cyberspace Policy Review, at 34 (Executive Branch report discussed in Paragraph 35(e)). That targeted condemnation has been based on unsubstantiated fear of selected companies with foreign national origin, rather than on evidence and facts.

40. Indeed, even though (as noted above) there are other technology companies owned by Chinese investors or operating in China, in recent years, Congress has singled out Huawei for special scrutiny and adverse action on the purported basis of unsubstantiated and largely unarticulated concerns, themselves apparently stemming from the belief that Huawei is owned, controlled, or subject to improper influence by the Chinese government.

[1] *See* Nokia Corporation, Stock Exchange Release, *Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture*, Nokia (May 18, 2017), https://tinyurl.com/y9vwu876; Nokia Corp., Annual Report (Form 20-F) (Mar. 22, 2018), available at https://bit.ly/2Aghem0; *China*, Ericsson, https://bit.ly/2Oxad9r (last visited Mar. 6, 2019) (noting that Ericsson "has several joint venture companies in China, including production companies").

41. As early as October 2010, four members of Congress sent a letter to the Chairman of the Federal Communications Commission (FCC), requesting information about the FCC's plans for protecting the security of U.S. telecommunications networks. Letter from Senator Jon Kyl et al. to Chairman Julius Genachowski (Oct. 19, 2010).[2]

a. The letter asserted that Huawei and another company, ZTE, were "aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure." *Id.*

b. The letter then stated that the members of Congress were "very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications network[s] . . . . This would pose a real threat to our national security." *Id.*

42. In light of such congressionally stated concerns, Huawei pledged in a February 2011 open letter to "remain open to any investigation deemed necessary by American authorities and . . . to cooperate transparently with all government agencies." Huawei Open Letter from Ken Hu, Deputy Chairman of Huawei Technologies, Chairman of Huawei USA, at 5 (Feb. 2011).[3] At the time, Huawei stated that it "ha[d] faith in the fairness and justness of the United States." *Id.* at 6. It further stated that it "believe[d] the results of any thorough government investigation [would] prove that Huawei is a normal commercial institution and nothing more." *Id.*

[2] Available at https://www.hsgac.senate.gov/media/minority-media/congressional-leaders-cite-telecommunications-concerns-with-firms-that-have-ties-with-chinese-government.

[3] Available at http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

43. In early 2011, the House Permanent Select Committee on Intelligence ("Committee") determined that, "without a full investigation into [Huawei's] corporate activities, the United States could not trust its equipment and services in U.S. telecommunications networks." U.S. House of Representatives, Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, at iv (Oct. 8, 2012) ("HPSCI Report").[4]

44. In response, Huawei made officials available to Congress in February 2012 for "extensive interviews." HPSCI Report at 8. House Committee staff interviewed Huawei executives at Huawei's corporate headquarters in Shenzhen, China, including John Suffolk, Huawei's Global Security Officer, and also toured Huawei's headquarters, "reviewed company product lines, and toured a large manufacturing factory." *Id.* at 8–9. The Rotating Chief Executive Officer, the Secretary of the Board, other corporate executives, and former and present employees also sat for "extensive interviews" lasting for "hours." *Id*. at v, 8, 10.

45. In May 2012, Committee members, including Representatives Devin Nunes, Michele Bachmann, Dutch Ruppersberger, and Adam Schiff, met with Ren Zhengfei, founder and CEO of Huawei, in Hong Kong. *Id.* at 9.

46. On September 13, 2012, the Committee held a congressional hearing at which a Huawei representative testified. *Id.*

47. In October 2012, the Committee published the HPSCI Report. In the report, the Committee admitted that it could "not prove wrongdoing" by Huawei. *Id.* at vi. Nonetheless, the Committee insisted that Huawei had not proved its own innocence, because it had failed to

[4] Available at https://fas.org/irp/congress/2012_rpt/huawei.pdf.

"provide greater details that would explain its relationships with the Chinese government in a way that would alleviate security concerns." *Id.* at 22.

48. The report specifically attributed the alleged security threat posed by Huawei equipment and services to Huawei's alleged relationship with, and alleged potential to be controlled by, the Chinese government. But the report cited no evidence that any equipment manufactured or services provided by Huawei had ever posed a national security risk. Nor did it cite any evidence that the Chinese government owned or controlled or was connected to Huawei, such that it could uniquely influence Huawei in any way.

49. Further, despite a lack of actual evidence that Huawei was connected to the Chinese government, much less that it had engaged in "wrongdoing" (at page vi) or that its equipment and services posed a security threat, the report recommended (at page 45) that "U.S. government systems, particularly sensitive systems, should not include Huawei . . . equipment, including in component parts," and, "[s]imilarly," that "government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude . . . Huawei equipment in their systems."

IV. THE 2019 NDAA

50. No statutory action was taken to implement the Committee's recommendations between 2012 and 2017.

51. In 2017, however, notwithstanding the lack of evidence against Huawei—and in disregard of the Executive Branch's recommendation to adopt a "broad, holistic approach to risk management" (Cyberspace Policy Review, at 34)—Congress enacted a statutory provision, as part of the National Defense Authorization Act for Fiscal Year 2018, that prohibited the Department of Defense from using specified Huawei equipment to carry out (1) "the nuclear deterrence mission of the Department," or (2) "the homeland defense mission of the Department,

including with respect to ballistic missile defense." Pub. L. No. 115-91, § 1656(a)–(b)(1), (c)(3)(A), 131 Stat. 1283, 1761–62 (2017) (identifying Huawei by name).

52. Further, on January 9, 2018, Representatives K. Michael Conaway and Liz Cheney introduced H.R. 4747, a bill to prevent all federal agency heads from procuring or obtaining, or contracting with any entity that uses, specified telecommunications equipment produced by Huawei. *See* H.R. 4747, 115th Cong. § 3 (2018).

53. On February 7, 2018, Senators Tom Cotton, John Cornyn, and Marco Rubio introduced S. 2391, a similar bill, in the Senate. *See* S. 2391, 115th Cong. (2018).

54. And on April 13, 2018, Representatives Mac Thornberry and Adam Smith introduced H.R. 5515, a bill that would become the 2019 NDAA.

55. On April 18, 2018, while these bills were pending, Senate Democratic Leader Chuck Schumer stated that "Huawei and ZTE are both state-backed companies. Their effort to enter the American market is a great example of how China attempts to steal our private data and intellectual property." 164 Cong. Rec. S2230 (daily ed. Apr. 18, 2018).

56. By May 15, 2018, when H.R. 5515 was reported to the full House by the House Committee on Armed Services, it contained provisions similar to those in H.R. 4747 and S. 2391. *See* H.R. 5515, 115th Cong. § 880 (as reported in House, May 15, 2018); H.R. Rep. No. 115-676, pt. 1, at 162–63 (2018).

57. On May 24, 2018, the House of Representatives passed its initial version of the 2019 NDAA.[5] That bill included conclusory and unsupported "[f]indings" stating that Huawei was "subject to state influence," H.R. 5515, 115th Cong. § 880(a)(4) (as passed by House, May 24, 2018), and "maintain[s] close ties to the [People's Liberation Army]," *id.* § 880(a)(1).

[5] Available at https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515eh.pdf.

58. The bill's proposed findings incorporated the HPSCI Report's recommendation that neither the government nor its contractors should work with Huawei. *See id.* § 880(a)(12); *supra* ¶ 49.

59. At the same time, the bill proposed to require agencies to submit plans detailing, among other things, "how the agency plans to deal with the impact of white label technology on its supply chain whereby the original manufacturer of technology is not readily apparent to a purchaser or user." *Id.* § 880(b)(2).

60. On June 4, 2018, the Senate received the bill from the House.

61. On June 13, 2018, Senator Cotton stated on the Senate floor: "These companies [*i.e.*, Huawei and ZTE] have proven themselves to be untrustworthy, and at this point, I think the only fitting punishment would be to give them the death penalty; that is, to put them out of business in the United States." 164 Cong. Rec. S3896 (daily ed. June 13, 2018). Senator Cotton called Huawei and ZTE "nothing more than extensions of the Chinese Communist Party"; stated that "Huawei's CEO was an engineer for the People's Liberation Army"; and asserted that Huawei's "greatest claim to fame is shamelessly stealing the secrets of American companies." *Id.*

62. Reflecting on the provisions of H.R. 5515, which he was helping to shape, *see* 164 Cong. Rec. S3362 (daily ed. June 7, 2018) (Sen. Cotton introducing Amendment 2514 to Amendment 2282 to H.R. 5515), Senator Cotton continued: "This is the first real, concrete action the United States has taken against Huawei and ZTE, but I and the Senators in this Chamber believe the death penalty is the appropriate penalty." 164 Cong. Rec. S3897 (daily ed. June 13, 2018).

63. Senator Chris Van Hollen added that "the Government of China exercises significant control over its telecommunications firms and . . . ZTE and Huawei have close and very longstanding ties to the government. We also know that China is one of the world's most active perpetrators of economic espionage and cyber attacks in the United States." *Id.*

64. Senator Rubio similarly stated in June 2018, that "we should put [Huawei] out of business," Marco Rubio, Press Release, *Rubio, Banks Raise Concerns of Chinese Espionage Through University Partnerships with Huawei* (June 20, 2018), [6] and that Huawei is a "Trojan horse" that "shouldn't be in business in the United States in any capacity." Gabriella Munoz, *Marco Rubio calls Chinese company Huawei a 'Trojan horse'*, The Washington Times (June 13, 2018).[7] He also tweeted that "[n]ow is a good time to start getting rid of your Huawei investments. Because while ZTE poses a very serious threat to the U.S. Huawei is 100 times worse."[8]

65. The Senate passed its version of H.R. 5515 on June 18, 2018,[9] and a conference committee was convened to produce a consensus bill.

66. On June 20, 2018, while Congress was considering the 2019 NDAA, Senators Cotton and Rubio, along with Representatives K. Michael Conaway, Liz Cheney, and Dutch Ruppersberger, sent a letter to Google expressing concern about its "strategic partnership" with Huawei, suggesting that the partnership could pose a "serious risk to U.S. national security," and

[6] Available at https://www.rubio.senate.gov/public/index.cfm/2018/6/rubio-banks-raise-concerns-of-chinese-espionage-through-university-partnerships-with-huawei.

[7] Available at https://www.washingtontimes.com/news/2018/jun/13/marco-rubio-calls-chinese-huawei-trojan-horse/.

[8] *See* Marco Rubio (@marcorubio), Twitter (June 13, 2018, 3:24 AM), https://twitter.com/marcorubio/status/1006844815433224192.

[9] Available at https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515pap.pdf.

criticizing Huawei for allegedly having "extensive ties with the Chinese Communist Party." Letter from Sen. Tom Cotton et al. to Sundar Pichai, CEO, Google (June 20, 2018).[10]

67. On June 27, 2018, Representative Ruben Gallego denounced "ZTE and Huawei Technologies" as "two bad apples" "owned by the Chinese Government" and noted that "[t]here is no partisan disagreement on this point." 164 Cong. Rec. H5805 (daily ed. June 27, 2018). He added that "we have seen that these companies . . . abuse and manipulate their placement in the market to attack sensitive American communications." *Id.*

68. The final version of the NDAA passed the House on July 26, 2018. Representative Smith applauded the bill's "very strict restrictions . . . on Huawei . . . to make sure they can't do business with the U.S. Government or with companies that do business with the U.S. Government." 164 Cong. Rec. H7700–01 (daily ed. July 26, 2018).

69. The final version of the NDAA passed the Senate on August 1, 2018.

70. On August 13, 2018, President Trump signed the 2019 NDAA into law. The President issued a signing statement highlighting numerous separation-of-powers concerns with, and objections to, the statute. The White House, Statement by President Donald J. Trump on H.R. 5515 (Aug. 13, 2018).[11]

71. The text of section 889 of the 2019 NDAA, as enacted in Public Law No. 115-232, is reproduced in the Appendix to this Complaint. In brief, section 889 prohibits federal agencies from (1) procuring covered Huawei equipment or services; (2) contracting with entities that use covered Huawei equipment or services; and (3) awarding grant or loan funds that will be

[10] Available at https://www.cotton.senate.gov/files/documents/180620_Congressional_letter_to_Mr_Sundar_Pichai.pdf.

[11] Available at https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-h-r-5515/.

used to procure covered Huawei equipment or services. The first prohibition formally takes effect one year after section 889's date of enactment; the second and third prohibitions take effect two years after enactment.

72. These prohibitions apply to the heads of all agencies in the Executive Branch. *See* 41 U.S.C. § 133 ("executive agency" means executive and military departments, as well as wholly owned government corporations and "independent establishment[s]" under 5 U.S.C. § 104(1)); 5 U.S.C. § 104(1) ("independent establishment" "in the executive branch").

73. These prohibitions bar Huawei from seeking or winning business with the federal government as to substantial categories of equipment and services—even as to agencies that have no significant connection to defense, information security, or national security, such as the National Rural Development Council within the Department of Agriculture, or the Bureau of Indian Affairs or the Fish and Wildlife Service within the Department of the Interior.

74. In addition to barring Huawei from providing covered equipment or services to federal agencies, these prohibitions impose a second layer of debarment that effectively disqualifies Huawei from selling covered equipment and services to thousands of private entities. Specifically, section 889's prohibitions effectively bar Huawei from seeking or winning substantial amounts of business with federal contractors or federal grant or loan recipients.

75. In 2015, the total value of federal contracts awarded was approximately $439.6 billion. Nat'l Contract Mgmt. Ass'n et al., Annual Review of Gov't Contracting, at 2 (2016 ed.). Given the size of this market, forcing Huawei's customers to choose between purchasing covered Huawei equipment and competing in the market for federal contracts is tantamount to preventing Huawei from doing business with federal contractors at all, with respect to covered Huawei equipment.

76. Section 889's prohibitions apply even where a federal contractor has a contract with an agency that has nothing to do with defense, information security, or national security.

a. Although a separate clause of the statute targets video surveillance equipment provided by certain companies "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes," Pub. L. No. 115-232, § 889(f)(3)(B), the clauses at issue here include no such "national security purposes" limitation.

b. For example, on its face, section 889 would effectively prohibit a federal contractor having contracts with the Department of Interior's Bureau of Indian Affairs or Bureau of Land Management, or with the Small Business Administration, from using Huawei equipment covered by the statute—even though those agencies have no security function.

77. Further, in an extraordinary example of overbreadth, section 889's prohibitions also apply even if a federal contractor uses Huawei equipment or services covered by the statute for a function that has nothing to do with the performance of the government contract.

a. For example, if an elevator company buys covered Huawei telecommunications equipment to use in its offices, section 889 would effectively preclude it from entering into a contract to repair elevators at the Department of Agriculture—even if the equipment in the offices has nothing to do with performance of the elevator repair contract.

78. Subject to a limited waiver provision, the NDAA's prohibitions on procurement and use of Huawei's covered telecommunications equipment and services are irrevocable.

a. With respect to most companies, the statute provides that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, may designate an entity as "owned or controlled by, or otherwise connected to, the government of [the People's Republic of China]" if he or she "reasonably believes" that such a designation is accurate. *Id.* § 889(f)(3)(D). That designation is then subject to revision or revocation if the relevant facts change.

b. But as to Huawei and one other named entity, even if the Secretary of Defense, the FBI Director, and the Director of National Intelligence definitively conclude that Huawei is not owned or controlled by, or otherwise connected to, the Chinese government, the prohibitions on the use of covered equipment and services would continue in force.

V. AGENCIES TAKE ACTION TO IMPLEMENT THE 2019 NDAA

79. On October 17, 2018, Huawei USA sent letters to Defendants DeVos, Perdue, and Wilkie, and to then-Secretary of the Interior Ryan Zinke, requesting their respective agencies' guidance regarding their implementation of the 2019 NDAA. The letters summarized section 889's prohibitions regarding Huawei, and explained that, while the prohibitions were not yet effective, they were of "enormous concern to Huawei and its customers," and were "already having negative effects on them." The letters then requested that, in accordance with 5 U.S.C. §§ 553, 555, and 28 U.S.C. § 530D, and applicable provisions of the Code of Federal Regulations (*see* 6 C.F.R. § 3.1–9; 7 C.F.R. § 1.28; 43 C.F.R. § 14.1–4), the agencies issue guidance, a rule, or an order confirming that they would decline to implement section 889 of the NDAA as it applies to Huawei, because it conflicts with the United States Constitution. The

letters specifically requested a response as soon as possible, and in any event no later than November 15, 2018. As of March 5, 2019, no substantive response has been received.

80. Also on October 17, 2018, Huawei USA sent letters to Defendants Acosta, Azar, Perdue, and Wilkie requesting their respective agencies' guidance regarding their implementation of the 2019 NDAA with reference to a specific Huawei matter related to the State of Georgia, with which all of these agencies have contracts. The letters summarized section 889's prohibitions regarding Huawei, and explained that Huawei had recently submitted a bid to the State of Georgia that had been denied because Georgia determined that Huawei was "non-responsible." The letters further explained that one reason for that determination was that, "according to Georgia, '[a]s of August 13, 2018,' Huawei technology would 'largely be banned from use by the U.S. government and government contractors' due to the 2019 NDAA, and many Georgia state entities receive substantial funding from the U.S. government." The letters also noted that Georgia had indicated that it would re-evaluate Huawei's proposal "'if and when[] the Federal government's ban on Huawei technology is lifted.'" In light of this situation, Huawei's letters requested "prompt guidance" on each agency's implementation of the 2019 NDAA. In particular, the letters requested that, in accordance with 5 U.S.C. §§ 553, 555, and 28 U.S.C. § 530D, and applicable provisions of the Code of Federal Regulations (*see* 6 C.F.R. § 3.1–9; 7 C.F.R. § 1.28), the agencies issue guidance, a rule, or an order confirming that they would decline to implement section 889 of the NDAA as it applies to Huawei, because it conflicts with the United States Constitution. The letters specifically requested a response as soon as possible, and in any event no later than November 15, 2018. As of March 5, 2019, no substantive response has been received.

81. Defendants Acosta, Azar, DeVos, Perdue, Wilkie, and Bernhadrt's failure to substantively respond to the letters described in paragraphs 79 and 80 constitute a "failure to act" (*see* 5 U.S.C. § 551(13)), which qualifies as "agency action" within the meaning of the Administrative Procedure Act, 5 U.S.C. § 500 *et seq*.

82. Also in October 2018, the U.S. Office of Management and Budget published the Fall 2018 Unified Agenda, which indicated that GSA, the National Aeronautics and Space Administration, and the Department of Defense "are proposing to amend the Federal Acquisition Regulation (FAR) to implement section 889" of the 2019 NDAA.[12] A Department of Defense list of open FAR cases indicates that the proposed amendment is currently being drafted.[13] The public has been invited to provide input on this effort to implement section 889. *See* Department of Defense, Defense Acquisition Regulations System, *Early Engagement Opportunity: Implementation of National Defense Authorization Act for Fiscal Year 2019*, 83 Fed. Reg. 42,883 (Aug. 24, 2018).

83. These official steps taken to amend the FAR and implement section 889 constitute "agency action" within the meaning of the Administrative Procedure Act, 5 U.S.C. § 500 *et seq*.

VI. INJURIES TO HUAWEI TRACEABLE TO THE 2019 NDAA

A. The 2019 NDAA Has Injured Huawei.

84. Even though the prohibitions in the NDAA do not formally become applicable until one or two years after enactment, depending on the particular provision at issue, section 889 is already causing Huawei actual, ongoing, and imminent injuries.

---

[12] *See* FAR Case 2018-017, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, RIN 9000-AN83, available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=9000-AN83.

[13] *See* Department of Defense, *Open FAR Cases as of 3/4/2019*, at 5, available at https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf.

85. Section 889 has injured Huawei by depriving it of its constitutional rights not to be subjected to a Bill of Attainder or a violation of Due Process.

86. In addition, Section 889 is causing, and will continue to cause (1) injury to Huawei's ability to compete on equal footing with its competitors; (2) actual, direct economic injury in the form of lost business opportunities and lost sales; and (3) injury to Huawei's business reputation and goodwill.

87. The pertinent provisions of section 889 of the 2019 NDAA have injured, and will continue to injure, Huawei's ability to compete on equal footing with its competitors.

a. Government contractors are part of Huawei's customer base. In recent years, Huawei USA has, either directly or through its distributors and resellers, done business or attempted to do business with federal government contractors. During this period, Huawei USA has sold or attempted to sell, whether directly or through its distributors and resellers, covered telecommunications equipment, such as routers and layer 3 switches, to such customers.

b. Huawei has ongoing direct or indirect relationships with customers who are federal government contractors. And in the absence of section 889 of the 2019 NDAA, it would expect to continue to do business with them in the future—including by selling them "covered telecommunications equipment." Consistent with its established past practices, Huawei would also expect, in the absence of section 889, to seek new business from government contractors.

c. In light of the enactment of section 889, however, Huawei's existing and potential future government contractor customers are being forced to choose

between continuing to bid on and carry out U.S. government contracts, and purchasing or using covered Huawei equipment and services. Beginning on section 889's relevant effective date, federal government contractors who use covered Huawei telecommunications equipment will no longer be eligible to enter into, or receive extensions or renewals of, contracts with executive agencies.

d. The forced choice imposed by section 889 has caused, and will continue to cause, Huawei concrete and particularized injury, and imminent future injury, because it prevents Huawei from competing for business with federal contractors on an equal footing with its competitors. Unlike Huawei, Huawei's competitors who are not expressly targeted by section 889 can sell equipment and services to federal contractors without such contractors having to choose between buying the equipment and doing business with the federal government.

e. This competitive injury began immediately upon the 2019 NDAA's enactment, has continued since then, and will continue into the future so long as section 889 remains in effect. Huawei's existing and potential future customers who are federal government contractors—like the vast majority of Huawei's customers—are considering the purchase of equipment, services, and systems with life spans of greater than two years (the effective date of some of the NDAA's prohibitions). The prospect of being prohibited from either using covered Huawei equipment and services on the one hand, or continuing to apply for federal contracts on the other hand, is therefore

affecting their decisions now. Customers do not want to invest money in equipment and services that will cause the loss of their ability to obtain, extend, or renew government contracts in less than two years.

f. This present reality has placed Huawei at a competitive disadvantage compared with other companies that are not subject to the same statutory restrictions in competing for these customers' business. Federal government contractors can purchase covered telecommunications equipment from, for example, Nokia Corporation ("Nokia"), Telefonaktiebolaget LM Ericsson ("Ericsson"), and other Huawei competitors without losing their ability to seek federal contracts after section 889's relevant effective date. The same disadvantage will extend to future purchasing decisions made by Huawei's current and potential customers who are (or would like to be) federal contractors. Indeed, as the two-year effective date approaches, customers and potential customers will feel the pressure of the choice between seeking federal contracts and using Huawei's covered products even more acutely.

g. Huawei has suffered a similar injury with respect to entities that receive grants and loans from the federal government. In recent years, Huawei has, directly or through its distributors and resellers, done business with federal grant recipients. During this period, Huawei USA has, directly or through its distributors and resellers, sold or attempted to sell covered telecommunications equipment, such as routers and layer 3 switches, to such customers. Based on this past record, Huawei USA anticipates continuing to

attempt to sell covered telecommunications equipment to federal grant and loan recipients.

h. But beginning on section 889's relevant effective date, federal grant and loan recipients will no longer be able to use federal grant or loan funds to procure or obtain covered Huawei telecommunications equipment. In contrast, even after section 889's relevant effective date, federal grant and loan recipients will be able to purchase such equipment from Nokia, Ericsson, and other Huawei competitors using federal grant or loan funds. The prohibition in section 889 thus places Huawei at a competitive disadvantage when marketing and attempting to sell covered telecommunications equipment to federal grant and loan recipients.

88. Huawei has also suffered actual, direct economic injury, and reasonably expects to continue to suffer further actual, direct economic injury, as a result of the pertinent provisions of section 889 of the 2019 NDAA. Customers have declined to sign contracts with Huawei or for Huawei equipment or services, ceased negotiations with Huawei or its resellers or representatives, or otherwise declined to do business with Huawei or purchase its equipment or services as a direct result of section 889. For example:

a. Huawei resellers have indicated that, since the enactment of the 2019 NDAA and as a result of its prohibitions, they have in some instances been unable to persuade their customers to purchase additional Huawei telecommunications equipment, potentially including routers or layer 3 switches, for their information technology needs. As a result, these resellers have acquired less Huawei equipment for resale to end-user customers than they otherwise would

have, and have paid Huawei less money than they otherwise would have, causing Huawei direct economic injury.

b. Huawei recently submitted a bid in response to a Request for Proposal (RFP) issued by the State of Georgia. That RFP was issued to establish one or more significant statewide contracts with one or more qualified suppliers who could provide enterprise infrastructure equipment and services—potentially including routers and other "covered telecommunications equipment" within the meaning of the NDAA—to Georgia. Based on past practices, Georgia had predicted that the total value of the contracts was likely to be approximately $20 million per year. Despite the fact that Huawei is highly qualified to provide such equipment, Georgia denied Huawei's bid on the basis that Huawei was "non-responsible." One reason for that determination was that, according to Georgia, "[a]s of August 13, 2018," Huawei technology would "largely be banned from use by the U.S. government and government contractors" due to the 2019 NDAA, and many Georgia state entities receive substantial funding from the U.S. Government. Georgia further indicated that it would be willing to re-evaluate Huawei's proposal "if and when[] the Federal government's ban on Huawei technology is lifted."

89. The pertinent provisions of section 889 of the 2019 NDAA have also injured, and will continue to injure, Huawei's reputation.

a. By suggesting that Huawei is owned or controlled by, or otherwise connected to, the Chinese government, and implying that Huawei equipment represents a security threat, section 889 causes immediate injury to Huawei's reputation.

b. Section 889 stigmatizes Huawei by suggesting that Huawei is subject to Chinese government influence, and implying that Huawei equipment is a security threat—thereby further suggesting that contracting or doing business with Huawei is unpatriotic and unwise.

c. These reputational injuries are underscored and amplified by numerous statements made by members of Congress, including Senators Cotton and Rubio, during the process of section 889's enactment. As described earlier, Senator Cotton stated on the Senate floor that Huawei has "proven [itself] to be untrustworthy," that it is "nothing more than [an] extension[] of the Chinese Communist Party," and that "the only fitting punishment would be to give [it] the death penalty." And Senator Rubio similarly stated that Huawei is a "Trojan horse" that "shouldn't be in business in the United States in any capacity." They also joined other members of Congress in expressing the view that cooperation between Huawei and other companies operating in the United States could pose a "serious risk to U.S. national security."

d. In addition, section 889's effective requirement that government contractors stop using covered Huawei equipment they have already purchased in order to be eligible for new federal contracts, or contract extensions or renewals, further injures Huawei's business reputation and goodwill, and exposes it to potential claims.

e. It is apparent that these reputational injuries are having concrete economic effects. For example, on February 29, 2019, the State of Vermont's Agency of Digital Services ("ADS") issued a directive to all Vermont state agencies,

departments, and other administrative agencies prohibiting them from acquiring, renewing contracts for, or using for any new purpose equipment manufactured by Huawei, based on the alleged "risks" presented by such equipment. *See* Memorandum from John Quinn, Secretary, Agency of Digital Services, State of Vermont regarding Cybersecurity Standard Update 19-01 (Feb. 19, 2019).[14] In support of this assessment and action, ADS specifically cites and relies upon the 2019 NDAA. *Id*.

90. The foregoing instances of concrete and particularized injury to Huawei, as well as the imminent future injuries Huawei faces, are directly traceable to the enactment of section 889, since that statute's prohibitions are a direct cause of the stated injuries.

B. Relief From This Court Will Remedy These Injuries.

91. By entering a judgment that the pertinent provisions of section 889 of the 2019 NDAA violate the Constitution and enjoining their implementation insofar as they apply to Huawei, this Court can remedy these injuries by eliminating the violation of Huawei's constitutional rights, removing significant barriers to Huawei's ability to compete on an equal footing with its competitors, preventing future economic injury created by section 889, and removing a cause of injury to Huawei's business reputation and goodwill.

92. Specifically, a judgment that section 889's prohibitions regarding procurement and use of covered Huawei equipment and services violate the Constitution, and enjoining the implementation of those provisions, would eliminate the Bill of Attainder and Due Process injuries caused by section 889, and rectify the violation of the separation of powers it represents.

[14] Available at https://digitalservices.vermont.gov/sites/digitalservices/files/documents/policy/ADS_Cybersecurity_Standard_Update_19-01.pdf.

93. Declaring these prohibitions unconstitutional and enjoining their implementation would also remove the categorical and irrebuttable prohibitions on government agencies' (1) procuring covered Huawei equipment or services; (2) contracting with entities that use covered Huawei equipment or services; and (3) awarding grant or loan funds that will be used to procure covered Huawei equipment or services. This in turn would permit Huawei to compete for business from government contractors and grant and loan recipients without facing the burdensome competitive disadvantage of requiring such customers to choose between purchasing covered Huawei equipment and services and retaining the ability to enter into contracts with, or to receive grants or loans from, the federal government.

94. Declaring these prohibitions unconstitutional and enjoining their implementation would also prevent future economic injury by permitting Huawei customers who are actual or potential government contractors or grant or loan recipients to purchase covered Huawei equipment and services without jeopardizing their ability to retain and compete for government contracts, or their ability to obtain federal grants or loans.

95. Declaring these prohibitions unconstitutional and enjoining their implementation would also eliminate a cause of Huawei's reputational injury.

FIRST CLAIM FOR RELIEF

(Bill of Attainder)

96. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and the paragraphs in the counts below as though set forth fully herein.

97. The Bill of Attainder Clause of the United States Constitution states: "No Bill of Attainder . . . shall be passed." U.S. Const. art. I, § 9, cl. 3.

98. Section 889 of the NDAA singles out Huawei Technologies and its subsidiaries and affiliates (including Huawei USA) for legislative punishment in two ways:

a. It singles out Huawei Technologies and one other entity from other businesses in general by effectively precluding the government, its contractors, and federal grant and loan recipients from using covered equipment and services produced or provided by Huawei and the other entity; and

b. It singles out Huawei Technologies and one other entity from other businesses supposedly controlled by, owned by, or otherwise connected to the Chinese government by permanently prohibiting use of their covered equipment and services directly in the statute rather than through discretionary executive adjudication subject to judicial review.

99. These features of section 889 of the NDAA constitute punishment as to Huawei in numerous respects. For example:

a. They subject Huawei to a burden—permanent debarment from providing certain products to the Federal Government, government contractors, and loan and grant recipients—that has traditionally been considered punitive. Excluding Huawei from the ability to pursue its ordinary business in the United States was an avowed purpose of section 889: as Senator Cotton (one of the advocates of section 889) candidly suggested, one primary objective of section 889 was to "punish[]" Huawei by "put[ting] [it] out of business in the United States."

b. They subject Huawei to burdens on the basis of its identity, instead of setting a general standard for the Executive and the courts to apply neutrally to Huawei and other companies on the basis of a factual record created after notice, a meaningful opportunity to be heard, and an opportunity for judicial review. As to most telecommunications companies, section 889 establishes a process in which the Secretary of Defense must "reasonably" determine whether a company is "owned or controlled by, or otherwise connected to" the Chinese government—a determination that is then subject to judicial review to assess whether the Secretary's determination was "[un]reasonabl[e]," arbitrary and capricious, or otherwise unlawful. But section 889 excludes Huawei from this process, and without evidence, opportunity for hearing, or Executive judgment subject to judicial review, instead categorically bans use of covered Huawei equipment and services—apparently based on Congress' own unfounded and unreviewable determination that Huawei is guilty of being owned, controlled by, or connected to the Chinese government, even though a congressional committee admitted in 2012 that it could not prove any such judgment.

c. They subject Huawei to a burden that is severe, permanent, and inescapable. As Senator Cotton suggested, the intent of section 889 is to impose on Huawei the corporate "death penalty" in the United States: it is nothing less than to put Huawei USA out of business and to exclude Huawei Technologies from the United States. And section 889's restrictions on procurement and use of covered Huawei equipment and services have no time limits, no expiration

date, and no mechanism for relief, even if the factual assumptions behind them are definitively proven false. Indeed, even if all Huawei entities were to leave China entirely, reincorporate elsewhere, and cease doing any business in China, section 889's prohibitions would remain in effect.

d. They call out Huawei by name in a way that brands it, its subsidiaries, and its affiliates as disloyal. The clear implication of the differential treatment imposed on Huawei, as compared to most other telecommunications companies, is that Huawei is a tool of the Chinese government whose equipment serves as a "Trojan Horse" that allows a hostile foreign government to infiltrate the United States. Indeed, numerous statements in section 889's legislative history—calling Huawei "untrustworthy," stating that it is a "state-backed compan[y]" with "close ties to the [People's Liberation Army]," and asserting that it is "nothing more than [an] extension[] of the Chinese Communist Party"—expressly so characterize Huawei.

e. They sanction Huawei in order to serve the punitive purpose of burdening a person in order to prevent the person from supposedly inflicting future harm—despite the fact that the Supreme Court has repeatedly held that specifically-targeted legislation motivated by such a purpose is unconstitutional.

f. They impose immense burdens that are disproportionate to any alternative non-punitive purpose, by disqualifying Huawei from doing business with the Federal Government and a substantial part of the U.S. economy, while imposing *no* legislative restrictions on many other telecommunications

companies that are from or do business in China. The burden section 889 imposes on Huawei is overbroad, barring it from selling covered equipment and services to contractors and grant and loan recipients whose use of Huawei equipment has nothing whatsoever to do with their performance of government contracts. At the same time, section 889 is substantially underinclusive, because it imposes no legislative restrictions whatsoever on equipment manufactured by Chinese government joint ventures with other telecommunications companies, or companies that have manufacturing facilities in China, embed components imported from China, or use software written by Chinese programmers. Congress thus made no serious or credible effort to ensure that section 889 was proportional to problems that it could legitimately seek to ameliorate. As noted earlier, the U.S. Government itself has repeatedly recognized that telecommunications supply chain risk is global, and that virtually all telecommunications infrastructure companies are potential sources of risk. Instead of focusing its energy on that widespread problem, Congress chose to scapegoat Huawei based on its alleged and unsubstantiated connections with the Chinese government.

g. They are based on and motivated by a blatant intent to punish, as demonstrated by the findings in the version of the bill passed by the House of Representatives, by statements made by Representatives and Senators when the bill was pending, and by Congress' repeated attacks against Huawei over many years. Senator Cotton candidly stated that a purpose of section 889 was to "punish[]" Huawei. Further, numerous statements in the legislative record

suggest that this desire to punish Huawei was motivated at least in part by an irrational fear that, because Huawei is a successful company organized in China, it must be subject to the direction and control of the Chinese government. The 2012 HPSCI Report admitted that the Committee could "not prove wrongdoing" by Huawei. Nonetheless, undeterred by this lack of evidence, the findings in the version of the 2019 NDAA passed by the House state that Huawei is "subject to state influence" and "maintain[s] close ties to the [People's Liberation Army]." And during the legislative process, members of Congress stated that Huawei was "nothing more than [an] extension[] of the Chinese Communist Party," and that Huawei had "extensive ties with the Chinese Communist Party"—suggesting that anti-Communist phobia also drove enactment of section 889.

h. They impose restrictions on Huawei while offering it no means to avoid or escape those restrictions, even if the allegations are shown to be false or if factual circumstances change.

i. They impose restrictions on Huawei while offering no procedural safeguards through which it can protect its rights. The statute gives Huawei no prior notice or opportunity to be heard; no statement of charges, much less of the evidence supposedly supporting the charges; and no fair mechanism for confronting that evidence and those charges.

j. They single out Huawei for legislatively imposed restrictions even though neither Huawei company constitutes a legitimate class of one. Indeed, by directing the Secretary of Defense to identify other companies that are "owned

> or controlled by, or otherwise connected to, the [Chinese] government," section 889 itself effectively *concedes* that the concerns that led to the enactment of the statute are posed by an open-ended class of companies, not just by a fixed "class" of one or two companies. This concession is confirmed by the Executive Branch's (and, sometimes, Congress' own) recognition that telecommunications supply-chain risks are global, and affect or have the potential to affect virtually all telecommunications companies, no matter their country of origin.

100. As legislation that selectively targets Huawei Technologies and Huawei USA and imposes punishment on them, the pertinent provisions of section 889 of the 2019 NDAA are an unconstitutional bill of attainder.

SECOND CLAIM FOR RELIEF

(Due Process)

101. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and the paragraphs in the counts below as though set forth fully herein.

102. The Fifth Amendment's Due Process Clause states: "No person shall . . . be deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

103. The Due Process Clause prohibits selective deprivations of liberty.

a. The Due Process Clause allows the Government to deprive a person of liberty in accordance with general laws, but not by selective enactments. *See, e.g.*, N. Chapman & M. McConnell, Due Process as Separation of Powers, 121 Yale L.J. 1672, 1734 (2012).

b. The Supreme Court has repeatedly stated that a legislative deprivation of liberty is constitutional only if it is imposed in accordance with general rules. *See, e.g.*, *Hurtado v. California*, 110 U.S. 516, 535–36 (1884); *United States v. Winstar Corp.*, 518 U.S. 839, 897–98 & n.43 (1996) (plurality).

104. Section 889 of the 2019 NDAA singles out Huawei (and one other entity) through selective enactment and deprives it of liberty.

a. Section 889 of the NDAA deprives Huawei of liberty by precluding it as a matter of law from selling covered equipment and services to federal agencies, contractors, and grantees.

b. Section 889 also deprives Huawei of liberty by stigmatizing it, declaring that it is subject to Chinese government influence. It does this despite the fact that, in the 2012 HPSCI report (on which the 2019 NDAA relies), a congressional committee admitted that it could not prove that Huawei had connections to the Chinese government or that it was a security threat. Rather than taking this conclusion to heart and focusing on holistically addressing the global supply chain risk by setting forth general standards, applicable to *all* companies that have connections with China, that could be implemented by Executive and judicial fact-finding, Congress doubled down on its unsupported allegations and irrationally scapegoated Huawei. The resulting stigma has the legal effect of burdening Huawei and precluding it from selling covered equipment and services to federal agencies, contractors, and grantees; and the practical effect of discouraging other entities across the United States from doing business with Huawei.

105. Moreover, section 889 deprives Huawei of these liberty interests by pure legislative fiat, referencing the unsupported conclusions in the 2012 HPSCI report and adopting them as "findings" in an early version of the bill, without giving Huawei any pre-deprivation opportunity to be heard, present evidence, or defend itself. This is the antithesis of the Due Process Clause's basic procedural protections of notice and an opportunity to be heard.

106. This specific legislative targeting, which deprives Huawei of its liberty, without proper pre-deprivation process, is unconstitutional under the Fifth Amendment's Due Process Clause.

THIRD CLAIM FOR RELIEF

(Separation of Powers)

107. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and the paragraphs in the counts below as though set forth fully herein.

108. The Constitution grants Congress only limited, enumerated "legislative powers," U.S. Const. art. I, § 1, and confers the "executive" and "judicial" powers on the President and the courts, respectively, *id.* art. II, § 1, cl. 1 (executive); *id.* art. III, § 1 (judiciary).

109. The limited, enumerated legislative powers encompass only the power to make legislative rules, not the power to apply legislative rules to individuals, because the power to apply legislative rules to individuals constitutes the exercise of executive and/or judicial power. *See, e.g.*, *Fletcher v. Peck*, 10 U.S. (6 Cranch) 87, 136 (1810) (Marshall, C.J.); *INS v. Chadha*, 462 U.S. 919, 966 (1983) (Powell, J., concurring in the judgment); *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 241 (1995) (Breyer, J., concurring in the judgment).

110. Section 889 of the NDAA is an unconstitutional exercise of executive and/or judicial power insofar as it legislatively prohibits purchase or use of covered Huawei equipment and services.

a. It singles out Huawei (and one other entity) for adverse treatment based on a specific congressional adjudication of its alleged connection to the Chinese government, and, therefore, its fitness to provide covered equipment and services to the government and its contractors and loan and grant recipients. Rather than announcing a general rule about the kinds of characteristics that would preclude a company from providing equipment and services to the federal government and its contractors and grant and loan recipients, section 889 imposes a legislative adjudication, decreeing that Huawei may not provide such equipment and services.

b. Although the statute tasks the Secretary of Defense with determining whether other entities are owned or controlled by, or otherwise connected to, the Chinese government, and allows judicial review of any such determination, in Huawei's case, the statute denies the Secretary and the courts any such authority, and instead itself specifies that procurement and use of Huawei's equipment and services is proscribed. This usurps functions properly committed to the Executive and Judiciary, and deprives Huawei of the structural protections available when such functions are exercised by their constitutionally-assigned branches, such as opportunities for executive consultation and subsequent judicial review, and the possibility of reconsideration.

111. Section 889 thus violates the Constitution's Vesting Clauses and resulting separation of powers.

PRAYER FOR RELIEF

112. **WHEREFORE**, Plaintiffs respectfully pray for an order and judgment:

a. Declaring that sections 889(a)-(b), (f)(3)(A), and (f)(3)(C) of the 2019 NDAA, insofar as they apply to Huawei Technologies and its subsidiaries and affiliates, violate the Bill of Attainder Clause of the United States Constitution.

b. Declaring that sections 889(a)-(b), (f)(3)(A), and (f)(3)(C) of the 2019 NDAA, insofar as they apply to Huawei Technologies and its subsidiaries and affiliates, violate the Due Process Clause of the Fifth Amendment to the Constitution.

c. Declaring that sections 889(a)-(b), (f)(3)(A), and (f)(3)(C) of the 2019 NDAA, insofar as they apply to Huawei Technologies and its subsidiaries and affiliates, contravene the Constitution's Vesting Clauses and the resulting separation of powers.

d. Enjoining the implementation of sections 889(a)-(b), (f)(3)(A), and (f)(3)(C) of the 2019 NDAA, insofar as they apply to Huawei Technologies and its subsidiaries and affiliates.

e. Awarding any and all other relief, including costs, as the Court deems just and proper in these circumstances.

Dated: March 6, 2019

Respectfully submitted,

/s/ Clyde M. Siebman
Clyde M. Siebman

Clyde M. Siebman
TX Bar No. 18341600
Michael C. Smith
TX Bar No. 18650410
Elizabeth S. Forrest
TX Bar No. 24086207
SIEBMAN, FORREST, BURG & SMITH, LLP
Federal Courthouse Square
300 North Travis Street
Sherman, TX 75090
(903) 870-0070
clydesiebman@siebman.com
michaelsmith@siebman.com
elizabethforrest@siebman.com

Andrew D. Lipman (D.C. Bar No. 280123)*
Russell Blau (D.C. Bar No. 366697)*
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, NW
Washington, DC 20004
(202) 739-6033
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com

Counsel for Plaintiffs

Glen D. Nager (D.C. Bar No. 385405)*
Ryan J. Watson (D.C. Bar No. 986906)*
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001
(202) 879-3939
gdnager@jonesday.com
rwatson@jonesday.com

Counsel of Record

**Pro hac vice* motions forthcoming

APPENDIX

SEC. 889. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

(a) PROHIBITION ON USE OR PROCUREMENT.—(1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(2) Nothing in paragraph (1) shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(b) PROHIBITION ON LOAN AND GRANT FUNDS.—(1) The head of an executive agency may not obligate or expend loan or grant funds to procure or obtain, extend or

renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain the equipment, services, or systems described in subsection (a).

(2) In implementing the prohibition in paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs, including the heads of the Federal Communications Commission, the Department of Agriculture, the Department of Homeland Security, the Small Business Administration, and the Department of Commerce, shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

(3) Nothing in this subsection shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) EFFECTIVE DATES.—The prohibition under subsection (a)(1)(A) shall take effect one year after the date of the enactment of this Act, and the prohibitions under subsections (a)(1)(B) and (b)(1) shall take effect two years after the date of the enactment of this Act.

(d) WAIVER AUTHORITY.—

(1) EXECUTIVE AGENCIES.—The head of an executive agency may, on a one-time basis, waive the requirements under subsection (a) with respect to an entity that requests such a waiver. The waiver may be provided, for a period of not more than two years after the effective dates described in subsection (c), if the entity seeking the waiver—

(A) provides a compelling justification for the additional time to implement the requirements under such subsection, as determined by the head of the executive agency; and

(B) submits to the head of the executive agency, who shall not later than 30 days thereafter submit to the appropriate congressional committees, a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the entity's systems.

(2) DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may provide a waiver on a date later than the effective dates described in subsection (c) if the Director determines the waiver is in the national security interests of the United States.

(f) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Financial Services, the Committee on Foreign Affairs, and the Committee on Oversight and Government Reform of the House of Representatives.

(2) COVERED FOREIGN COUNTRY.—The term "covered foreign country" means the People's Republic of China.

(3) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES.—The term "covered telecommunications equipment or services" means any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(C) Telecommunications or video surveillance services provided by such entities or using such equipment.

(D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(4) EXECUTIVE AGENCY.—The term "executive agency" has the meaning given the term in section 133 of title 41, United States Code.